DISASTER, RECOVERY, OR HOW TO REDUCE LOSSES
IT SECURITY ACADEMY
www.SecAcademy.com

MINIMIZING ATTACK AND INTRUSION DAMAGE

DISASTER RECOVERY PLANS are an essential part of security policies

THE QUICKER A LAUNCHED attack is discovered, the easier it is to stop and (if it has managed to compromise the system) minimize damage and bring the system back to functionality

DISASTER RECOVERY PLANS should be designed by the most experienced administrator and tested by the least experienced user in a company

ENSURING CONTINOUS AVAILABILITY

Network Load Balancing

NETWORK LOAD BALANCING improves the availability and scalability of network services like web servers, FTP servers, firewalls, proxy servers and report servers

A PROTECTED SERVICE in this case is running on more than one computer, meaning there is a separate launched copy of the service in each of the hosts

NETWORK LOAD BALANCING is a function dividing incoming client requests between the networked hosts. As a result, each of them only processes a part of user requests

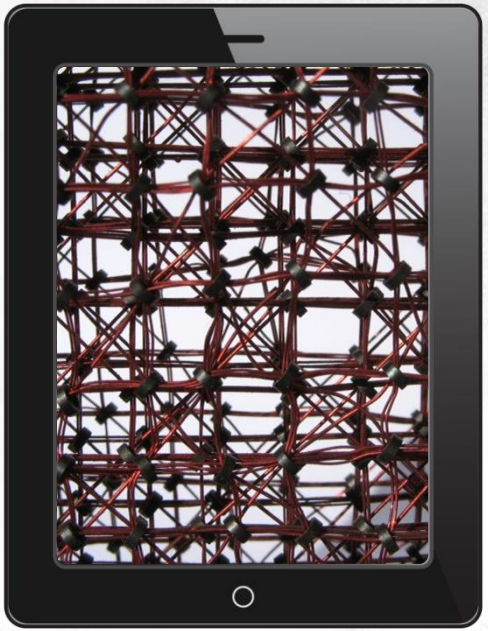
ENSURING CONTINOUS AVAILABILITY

Network Load Balancing

THE LOAD ON EACH host may be calibrated (by doing so you can increase the performance of the service). Network Load Balancing can direct all traffic to a single designated host

WHEN ONE HOST FAILS, incoming requests are automatically passed to the running computers. Because of this, a single host failure will hurt the performance of a service, but will keep it from becoming unavailable

UNLIKE FAILOVER CLUSTERS, services that are protected using NLB do not share data. Each host has its own copy of the data. As a consequence, if you want to allow users to modify it, it's necessary to sync the copies across the computers



ENSURING CONTINOUS AVAILABILITY

Failover Clusters

A NODE
(either physical or virtual) is a computer in a cluster

A PROTECTED SERVICE
(like a database server) is only running in a single active node. If the node becomes unavailable, the service fails over to another (passive) node

TWO NODES
are necessary to ensure continuous availability: one active and one passive node

ADDITIONAL CLUSTER
nodes are only needed if you have more services running in the cluster

ENSURING CONTINOUS AVAILABILITY

THE NAMES (PASSIVE AND ACTIVE) ARE SELF-EXPLANATORY:

THE ACTIVE NODE RUNS USER
requests and controls the access to files kept in shared storage Failover Clusters

THE PASSIVE NODE IS INACTIVE
and doesn't have access to the files. Its role is to monitor the availability of the active node

ENSURING CONTINOUS AVAILABILITY

Failover Clusters

When you activate a cluster, the nodes in it communicate with each other over a network. Because of this, setting changes in the active mode will be automatically synced. Each node should have at least two NICs, with one card connected to a private network, and the other connected to a public network

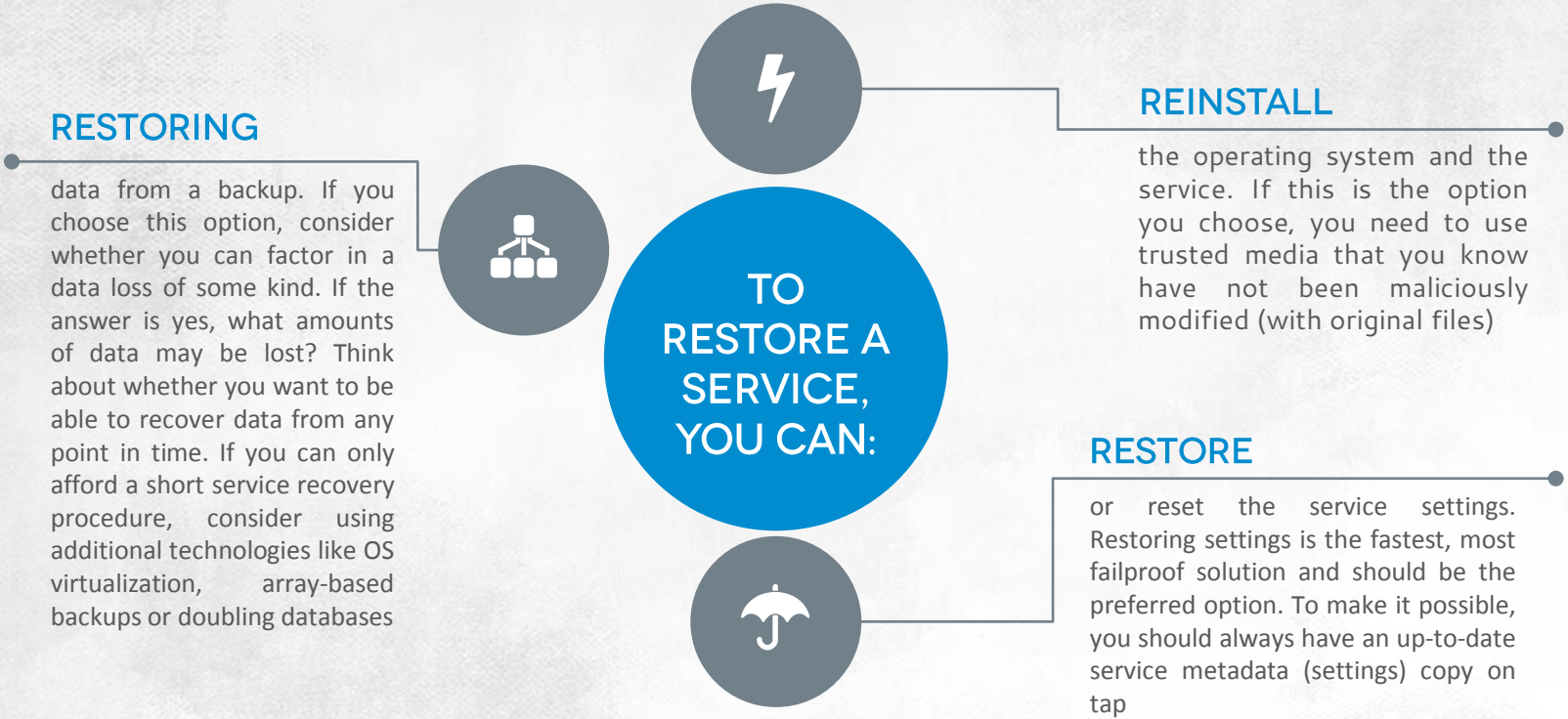
THE PRIVATE NETWORK

will only be used for inter-node communications like checking on the availability of the active node. To do this, the active node sends a signal (heartbeat) to the passive node at regular intervals

THE PRIVATE NETWORK

The public network allows clients to access the protected service

RESTORING A SERVICE


TO RESTORE A SERVICE, YOU CAN:
RESTORING
data from a backup. If you choose this option, consider whether you can factor in a data loss of some kind. If the answer is yes, what amounts of data may be lost? Think about whether you want to be able to recover data from any point in time. If you can only afford a short service recovery procedure, consider using additional technologies like OS virtualization, array-based backups or doubling databases
REINSTALL
the operating system and the service. If this is the option you choose, you need to use trusted media that you know have not been maliciously modified (with original files)
RESTORE
or reset the service settings. Restoring settings is the fastest, most failproof solution and should be the preferred option. To make it possible, you should always have an up-to-date service metadata (settings) copy on tap

THREAT DISCOVERY

The security log may be set to record both failed and successful attempts by users to run some operations

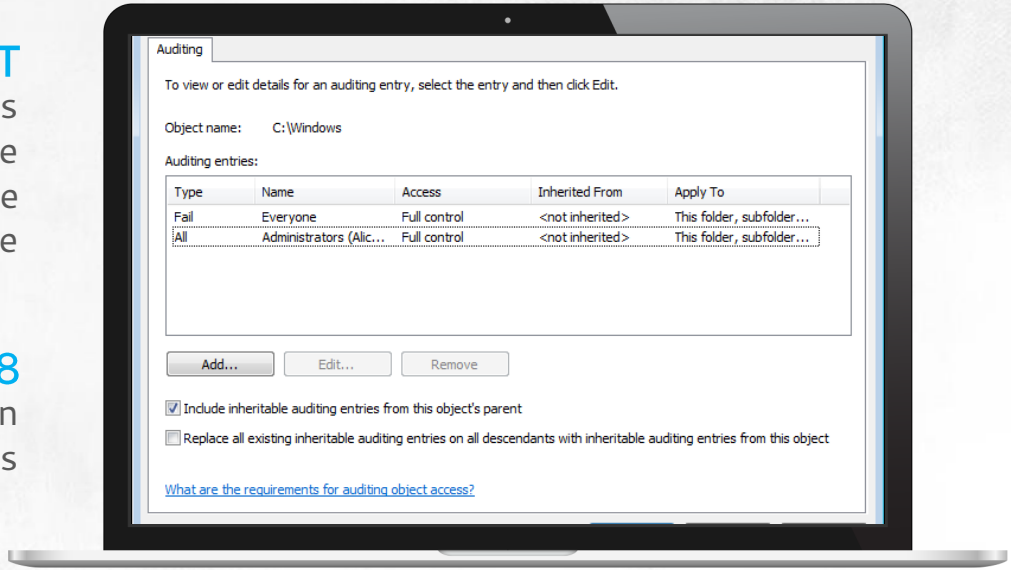
The security log is not on by default in earlier versions of Windows

CATEGORY	DESCRIPTION
AUDIT OBJECT ACCESS	LOGGING USER ACCESSING SACL OBJECTS LIKE FILES AND FOLDERS ON NTFS DISKS AND PRINTERS.
AUDIT DIRECTORY SERVICE ACCESS	LOGGING USER ACCESSING ACTIVE DIRECTORY SERVICES LIKE ACCOUNTS, ORGANIZATIONAL UNITS OR GROUP POLICY.
AUDIT PROCESS TRACKING	LOGGING PROGRAMS EXECUTING EVENTS LIKE STOPPING A PROCESS OR STARTING A PROGRAM.
AUDIT PRIVILEGE USE	LOGGING ALL INSTANCES OF USING PRIVILEGE, FOR EXAMPLE TAKING OWNERSHIP OF A FILE.
AUDIT ACCOUNT MANAGEMENT	LOGGING USERS CREATING, DELETING OR MODIFYING AN ACCOUNT OR GROUP, FOR EXAMPLE DELETING AN ACCOUNT, DEACTIVATING AN ACCOUNT OR SETTING AND CHANGING PASSWORDS.
AUDIT LOGON EVENTS	LOGGING USER LOGONS AND LOGOUTS. FOR DOMAIN ACCOUNTS, THESE EVENTS WILL BE LOGGED BY A DOMAIN CONTROLLER, AND FOR LOCAL ACCOUNTS, BY A LOCAL COMPUTER.
AUDIT ACCOUNT LOGON EVENTS	LOGGING USER AUTHENTICATION REQUESTS ISSUED BY A DOMAIN CONTROLLER.
AUDIT SYSTEM EVENTS	LOGGING SHUTTING DOWN AND RESTARTING THE OPERATING SYSTEM AND OTHER SECURITY-RELEVANT EVENTS.
AUDIT POLICY CHANGE	LOGGING ALL INSTANCES OF MODIFYING USER PRIVILEGES, AUDIT POLICY OR TRUST POLICY.

THREAT DISCOVERY

ONCE YOU ENABLE AUDIT object access, specify the objects to be audited and users whose events should be logged in the security log, as well as determine the events to be audited

IN WINDOWS SERVER 2008 and newer systems you can enable Global Object Access Audit

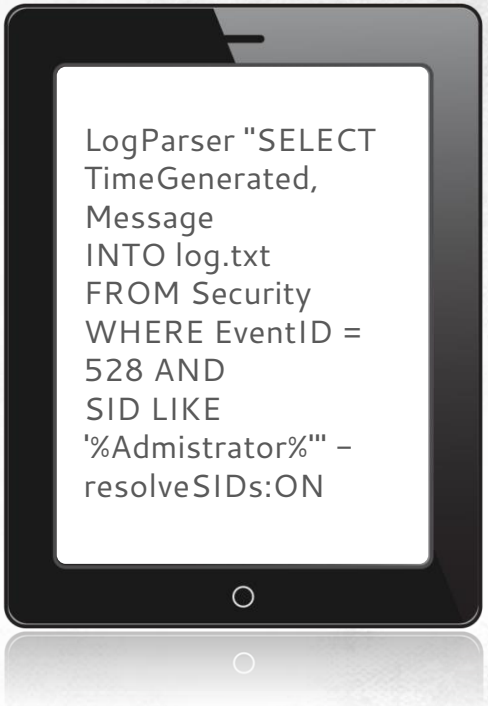


THREAT DISCOVERY

GOING OVER ALL THE DATA LOGGED WOULD BE TOO TIME-CONSUMING AND NOT EFFECTIVE ENOUGH TO DO MANUALLY

Log Parser, available at Microsoft Download, solves both these problems at once. It will allow you to:

- **SEARCH THROUGH**
  data using SQL commands
- **PRESENT DATA CULLED**
  from the logs as HTML reports
- **GROUP AND ANALYSE DATA**
  and present output as charts



THREAT DISCOVERY

The security log entries will allow you to:

DETECT

security policy breaches

DISCOVER

external attacks

INVESTIGATE

an attack and prepare avidence

THREAT DISCOVERY

YOU CAN AUDIT USERS trying to access folders by monitoring event 560. The data you need to analyse failures include the Object Name attribute as well as Primary User Name and Client User Name

THREAT DISCOVERY

698

changing Active Directory controller restoring password. You'll find the name of the user who tried to make this change in the User Name field, while the IP address of this user's computer is under the Workstation IP attribute

635 TO 638

logged in the case of a modification of local groups

624

logged when a new account is created. You'll find the name of the user account who performed this operation under Primary User Name

627

reported when someone tries to change a user password. The name of the modified account is the value of Target Account Name, while to see which user changed the password, look for the Primary Account Name attribute

628

resetting user password using administrative tools

631 TO 634

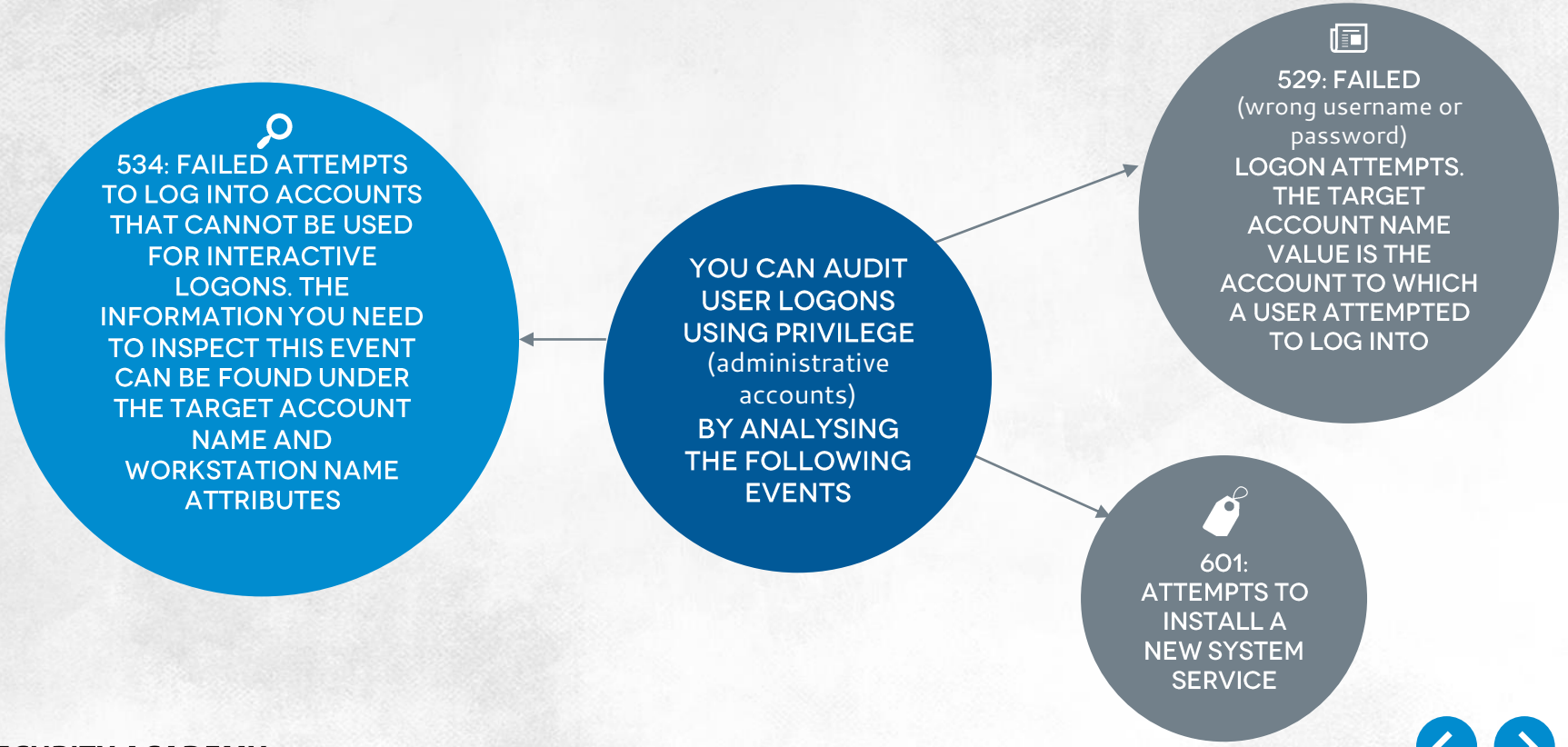
these events are logged in the case of a modification of global groups

THREAT DISCOVERY

An attacker may attempt to hide a security policy breach by diverting the attention of the admin or by changes made to audit policy (turning off the auditing of some events) or by a deletion of the security log file. You can discover these operations by auditing the following events:

- **516:** indicates that the log is full and new events cannot be audited. Increase the size of the log file or copy its content and clear the log
- **517:** occurs when the log is cleared. The Client User Name attribute gives you the name of the user who performed this operation
- **520:** a change of the system time. All events saved in logs come with the time of occurrence, which is the local system time, so this event may mean your auditing system is being cheated, for example to gain an alibi. You can find the name of the user responsible for this under Client User Name
- **521:** a system error that causes the log to fail to record new events

THREAT DISCOVERY


534: FAILED ATTEMPTS TO LOG INTO ACCOUNTS THAT CANNOT BE USED FOR INTERACTIVE LOGONS. THE INFORMATION YOU NEED TO INSPECT THIS EVENT CAN BE FOUND UNDER THE TARGET ACCOUNT NAME AND WORKSTATION NAME ATTRIBUTES
YOU CAN AUDIT USER LOGONS USING PRIVILEGE (administrative accounts) BY ANALYSING THE FOLLOWING EVENTS
529: FAILED (wrong username or password) LOGON ATTEMPTS. THE TARGET ACCOUNT NAME VALUE IS THE ACCOUNT TO WHICH A USER ATTEMPTED TO LOG INTO
601: ATTEMPTS TO INSTALL A NEW SYSTEM SERVICE

THREAT DISCOVERY

Attempts to log into inactive (for example expired) or blocked accounts will log these events:

531

failed attempts to log into a blocked account. To see the name of the account, check Target Account Name. You'll get the name of the computer from which the logon was made under Workstation Name

532

failed attempts to log into inactive accounts

EXERCISE

File Authenticity Check

CHECKING SYSTEM
integrity using SigCheck

CONTROLLING FILE
checksums using ExactFile

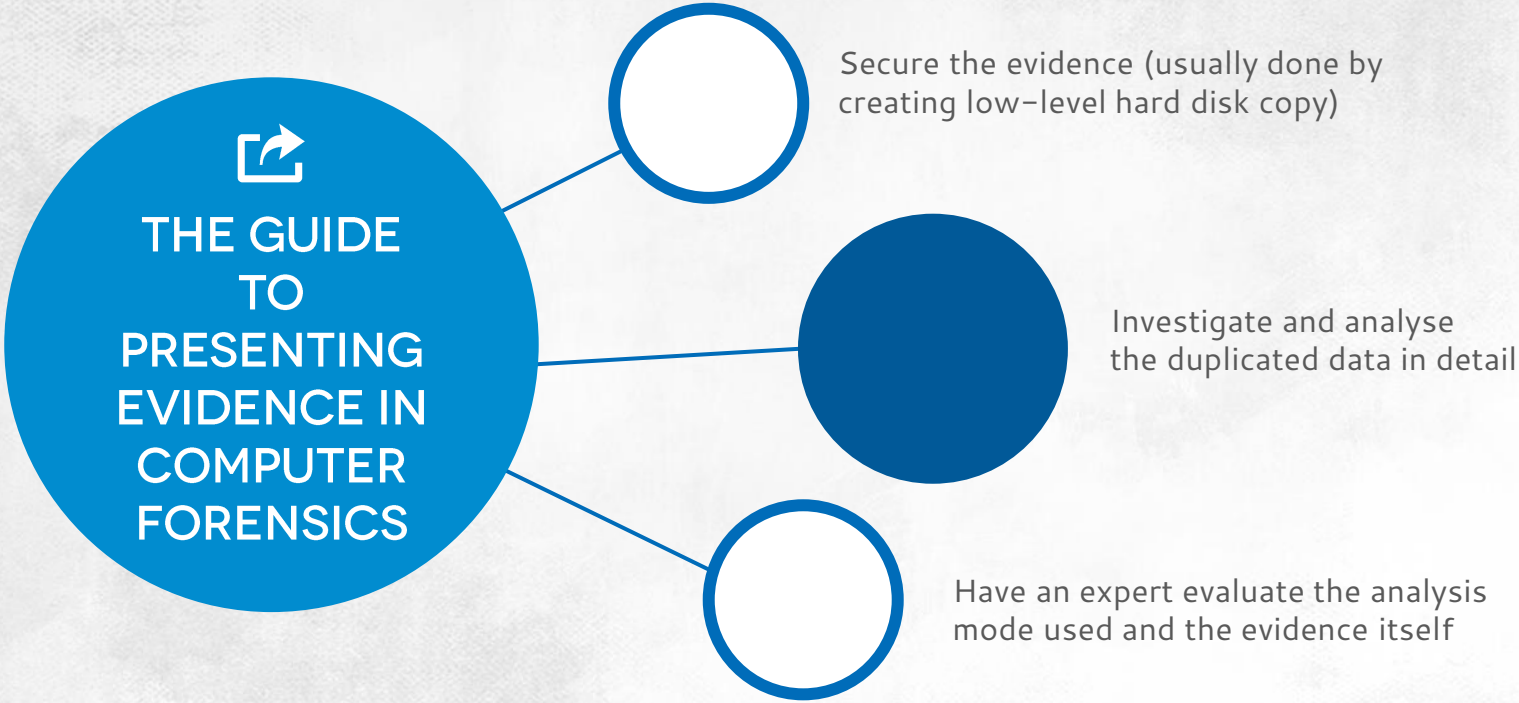
COLLECTING AND ANALYSING EVIDENCE

THE ROLE OF COMPUTER forensics is to secure and analyse the evidence of computer crimes

EVIDENCE CAN BE RETRIEVED from security logs, IDS logs or images of drives on compromised computers

Web Images Video News Maps Desktop more »
Search
All - 0 emails - 1 file - 0 web history - 0 chats - 0 other
Remove from Index | Sort by relevance
Sorted by date
Computer
Local Disk (C:)
Floppy Disk Drive (A:)
CD Drive (D:)
RESEARCHER-PC
WORKGROUP

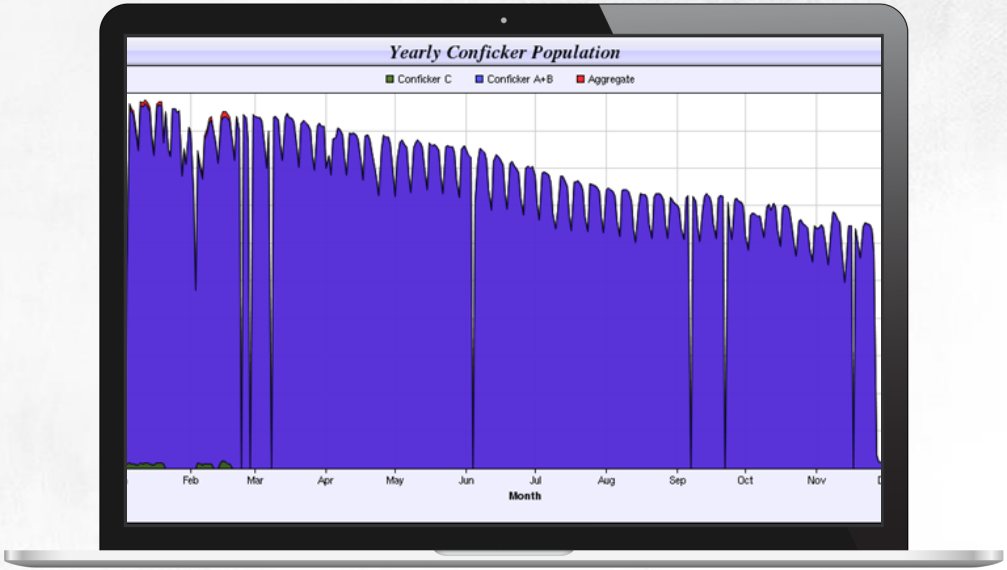
COLLECTING AND ANALYSING EVIDENCE


THE GUIDE TO PRESENTING EVIDENCE IN COMPUTER FORENSICS
Secure the evidence (usually done by creating low-level hard disk copy)
Investigate and analyse the duplicated data in detail
Have an expert evaluate the analysis mode used and the evidence itself

COLLECTING AND ANALYSING EVIDENCE

CONFICKER belongs to the self-propagating breed of viruses that don't need user interaction

CONFICKER targeted Windows systems. A month before the virus was detected, Microsoft shared a security update patching up a discovered vulnerability (MS08-067 was published October 2008)

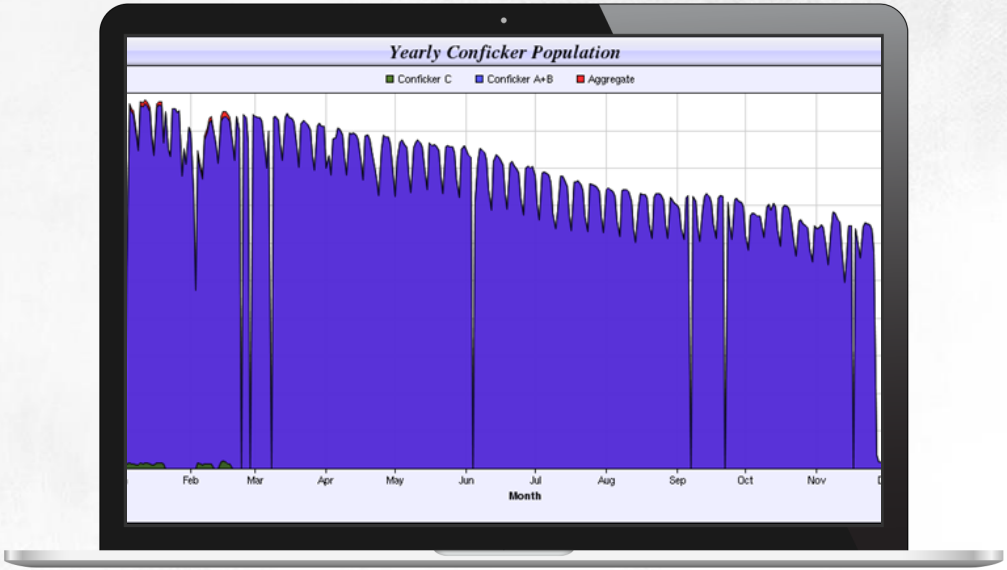


COLLECTING AND ANALYSING EVIDENCE

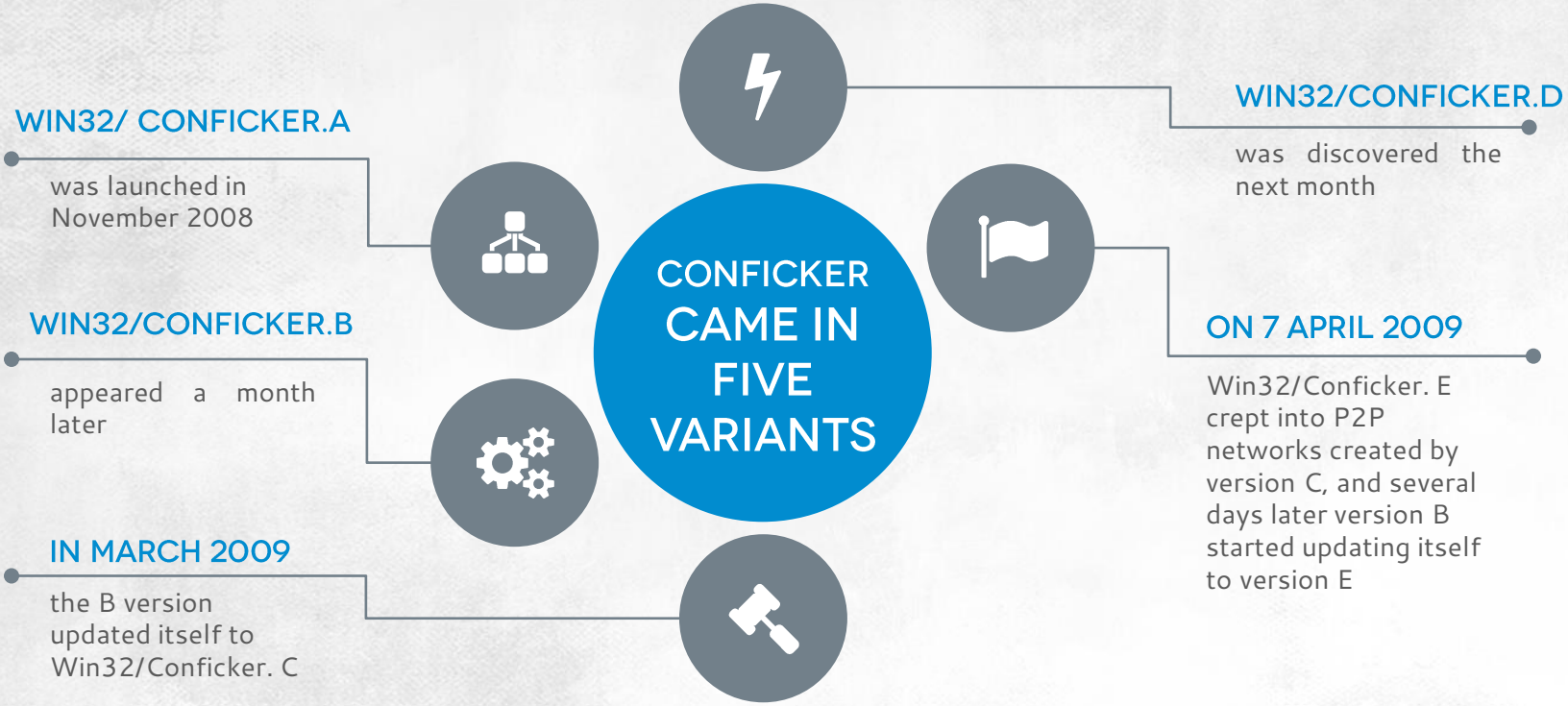
After the pandemic broke out, Microsoft shared a comprehensive guide to removing the worm (KB960027) and offered a reward (250,000 dollars) for help in identifying the creators of Conficker

Also known as Downadup, the name Conficker comes from the domain name trafficconverter.biz which computers infected with version A of the virus connected with:

((FIC)(CON)(ER) => (CON)(FIC)(+K)(ER) => CONFICKER.



CONFICKER: CASE STUDY


CONFICKER CAME IN FIVE VARIANTS
WIN32/ CONFICKER.A
was launched in November 2008
WIN32/CONFICKER.B
appeared a month later
IN MARCH 2009
the B version updated itself to Win32/Conficker. C
WIN32/CONFICKER.D
was discovered the next month
ON 7 APRIL 2009
Win32/Conficker. E crept into P2P networks created by version C, and several days later version B started updating itself to version E

CONFICKER: CASE STUDY

AN ADMINISTRATOR'S FIRST DUTY IS TO DISCOVER THE ATTACK IS OCCURRING

It was an easy task with Conficker
Since infected machines would make 500 connections with domains chosen randomly from a pool of 50,000 and attempted to spread to the other hosts in a system, there were obvious signs something was wrong:

- DOMAIN CONTROLLER load rose significantly and correlated with a significant drop in performance
- MANY USER ACCOUNTS were automatically blocked (as the virus attempted to crack user passwords)
- THERE WAS a noticeable decrease in performance in all network applications

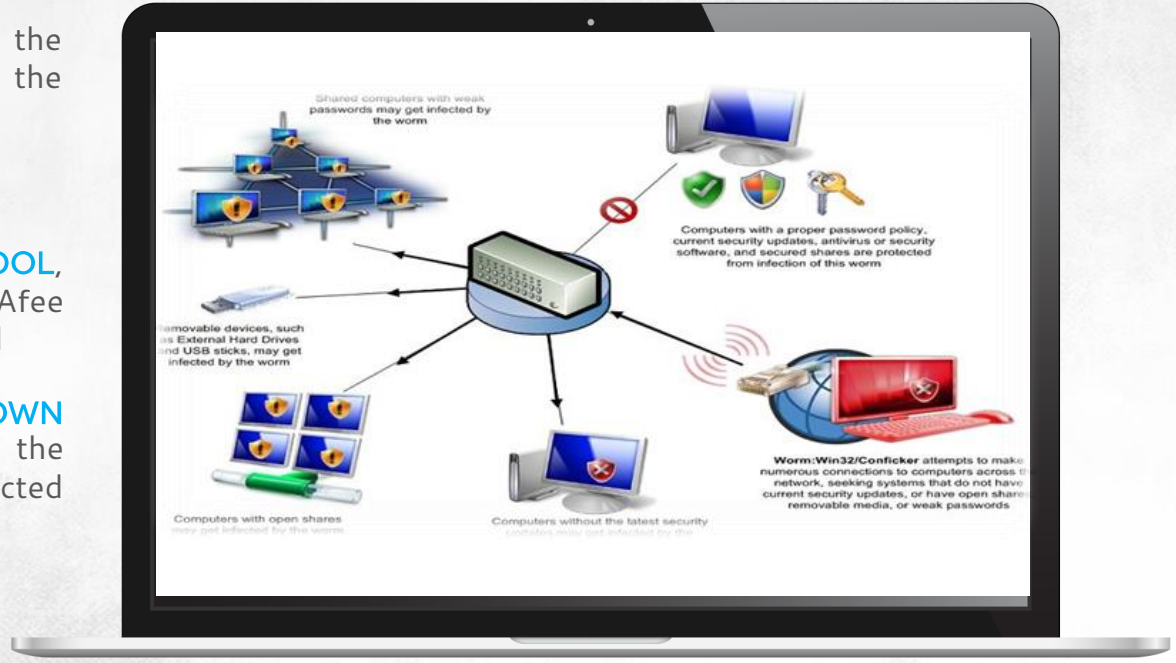
Moreover, if you remembered about updating antivirus scanners regularly, the programs reported finding a virus

CONFICKER: CASE STUDY

The next step is determining the attack scale and preventing the virus from spreading

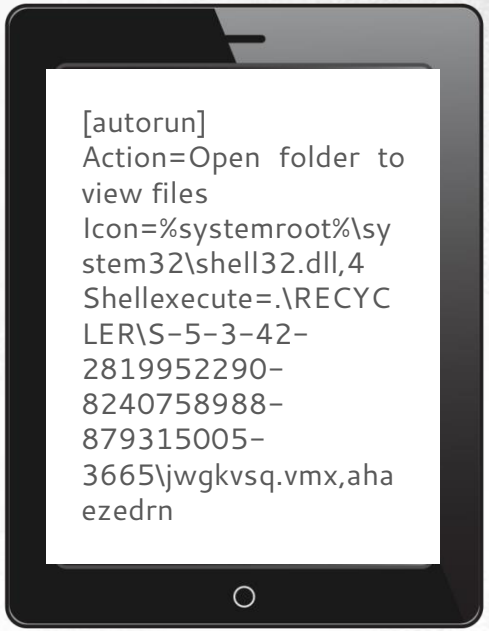
To do this, you could:

- **USE A DEDICATED TOOL**, for instance McAfee Conficker Detection Tool
- **USE WHAT WAS KNOWN** about the operation of the worm to identify infected computers on your own


Shared computers with weak passwords may get infected by the worm
Computers with a proper password policy, current security updates, antivirus or security software, and secured shares are protected from infection of this worm
Computers with open shares
Computers without the latest security
Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords

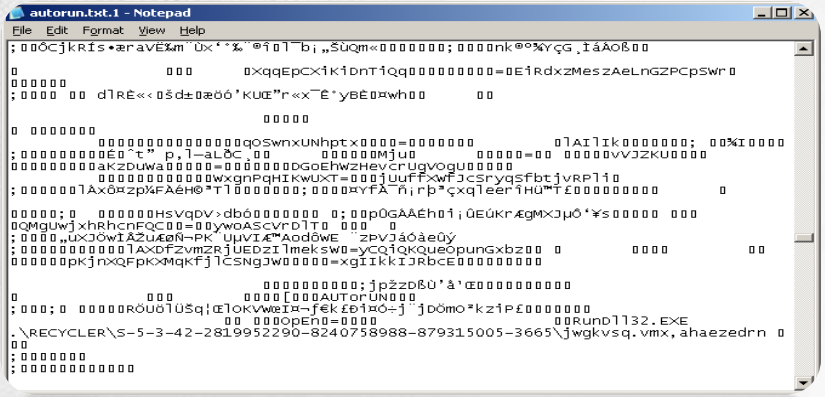
CONFICKER: CASE STUDY

The virus would modify the autorun.inf file to trick users into starting the infected file



CONFICKER: CASE STUDY

It would also save a hidden worm copy file on removable media



Removable Disk (E:)
Windows can perform the same action each time you insert a disk or connect a device with this kind of file:
Program
What do you want Windows to do?
Open folder to view files using the program provided on the device
Open folder to view files using Windows Explorer
Take no action
Always do the selected action.
OK
Cancel

ONCE STARTED, THE WORM WOULD CREATE A NEW SYSTEM SERVICE WITH A RANDOM NAME

HKLM\SYSTEM\CurrentControlSet\Services\{random}\Parameters\"ServiceDll" = "Virus File Location"

When you restarted your computer, the service would run automatically

CONFICKER: CASE STUDY

Spreading through Cracking Passwords

CONFICKER INCLUDED a popular password list to crack user passwords

BESIDES THE LIST, it used a simple mechanism to check if passwords are built on usernames. For example, if the username was James, Conficker would attempt to log into this account by trying james123, 123james, semaj and so on

THIS RESULTED IN massive account lockouts as a single compromised host in large systems could lock out even several thousand user accounts

A FAST AND GOOD WAY to detect which machines were infected was simply to see the IP addresses of computers responsible for the lockouts

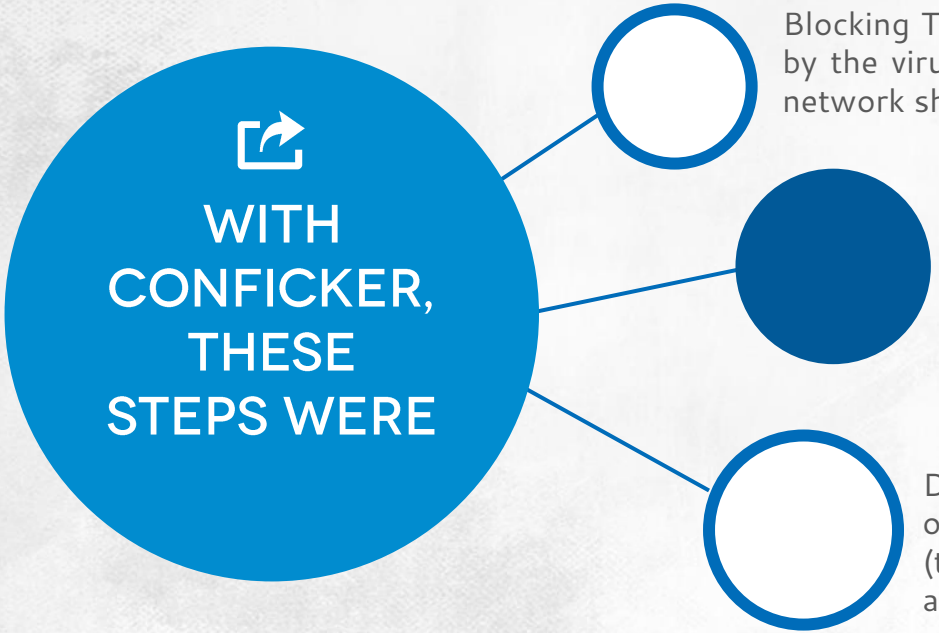
TO FIND THEM, you could fall back on a free tool suite available at Microsoft Download: Account Lockout and Management Tools. The suite included EventCombMT

IT WAS ENOUGH TO analyse the generated file using Log Parser to receive the IP addresses of infected computers

```
logparser -i:textline
"SELECT SUBSTR(Text,
LAST_INDEX_OF(Text,
'Address: ')) AS IPAddr
INTO addrs.csv
FROM *.txt"
```

CONFICKER: CASE STUDY

Simultaneously to assessing the attack territory, you need to take steps towards protecting the remaining computers



Blocking TCP port 445, which was used by the virus to spread itself using SMB network shares

Denying registry key (HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost) modification privileges using Group Policy (check out the knowledge base article 962007 at http://support.microsoft.com/kb/962007#Mitigationsteps to see how to edit the policy)

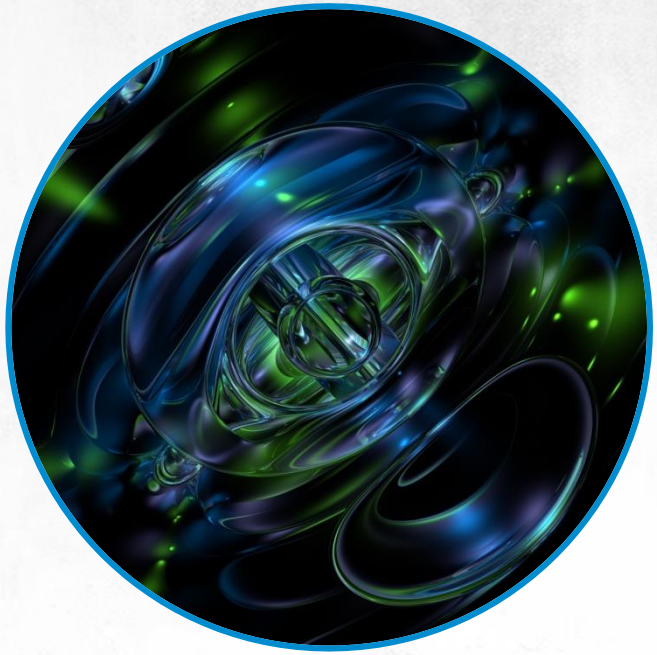
Disabling the automatic run of files on removable media (tips found in the article above)

CONFICKER: CASE STUDY

AFTER YOU STOP THE ATTACK FROM SPREADING, THE NEXT STEP IS TO REMOVE THE VIRUS FROM COMPROMISED MACHINES

In this case, you could use one of the several freely available tools, like Microsoft's malware removal tool, EConfickerRemover (ESET), D (Symantec), Stinger (MCAfee) or Kaspersky's Killer removal tool

YOUR LAST TASK IS MAKING SURE THAT THE MALWARE IS TRULY REMOVED FROM THE SYSTEM AND ENSURING SIMILAR ATTACKS WILL BE PREVENTED IN THE FUTURE



THANKS